REMARKS/ARGUMENTS

Claims 1-21 are pending in the present application. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 102, Anticipation

Claims 1, 8 and 15 stand rejected under 35 U.S.C. § 102 as being anticipated by Hutchison et al. (U.S. Patent No. 7,249,191 B1), hereinafter "Hutchison". This rejection is respectfully traversed.

For a prior art reference to anticipate in terms of 35 U.S.C. 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). "To establish inherency," the Federal Circuit recently stated, "the extrinsic evidence `must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.'" *In re Robertson*, 169 F.3d 743, 745 [49 USPQ2d 1949] (Fed. Cir. 1999); see also *Continental Can Co. U.S.A., Inc. v. Monsanto Co.*, 948 F.2d 1264, 1268 [20 USPQ2d 1746] (Fed. Cir. 1991). Such inherency may not be established by "`probabilities or possibilities.'" *Continental Can*, 948 F.2d at 1269 (quoting *In re Oelrich*, 666 F.2d 578, 581 [212 USPQ 323] (C.C.P.A. 1981)).

With respect to Claim 1, such claim recites "receiving a request for host information for a remote computer from a requestor wherein the request includes one of a host name or an Internet Protocol address and is received from the requestor", "identifying a media access control address *and a subnet mask* using the request" and "returning a response to the requestor, wherein the response includes the media access control address *and the subnet mask*" (emphasis added by Applicants). The cited reference does not teach specific steps of (1) identifying a *subnet mask* using a request that was received, or (2) **returning a response that includes a *subnet mask***.

In rejecting Claim 1, the Examiner states that it is inherent 'that subnet mask will be there along with MAC address or else the packet will be loss (sic) not knowing which network or which segment of the network it belongs to'. Applicants urge clear error in such inherency assertion, as one of the fundamental premises that the teachings of the cited reference are directed to is to provide a transparent platform that intercepts a file from a source across a first IP connection, and resends such file over a second TCP connection (Hutchinson Abstract). This redirection of the file from the first IP connection to a second IP connection is done using a specialized network address translation bridge. Importantly, this bridge 'spoofs' a client that wishes to retrieve a particular web page, by using an intervening gateway that intercepts the client's request for a MAC address of the device containing the desired web page, and *this gateway instead provides the client with its own MAC address* (col. 4, lines 18-23; Figure 8, element ARP

REPLY 10.0.0.1 = ABCD). Even more importantly, this intervening gateway is in the _same_ *subnet* as the client (gateway has IP address of 10.0.0.1 and client has IP address of 10.0.0.2 as clearly shown in Figure 8) so there is no issue with losing a packet by not specifying a subnet mask in response to the request for a MAC address, as the gateway 'spoofs' the client by providing *its own* MAC address *which is on the* _*same*_ *subnet as the client*. Thus, there is no reason or need for this spoofing gateway to also include a subnet mask in the response to the request for a MAC address, as both devices (gateway and client) are on the same subnet and thus such mask is not needed to ensure proper addressing between the client and the spoofing gateway. Therefore, the extrinsic evidence does not make it clear that the missing claimed feature (subnet mask being returning in a request) is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill in the art, as required by *In re Robertson,* supra.

Quite simply, inclusion of such a subnet mask (as claimed) would needlessly consume valuable system bandwidth by transmitting useless information that is not needed – somewhat akin to including a country code when dialing a local, non-international phone call, it's just not done because it is not needed. Therefore, whether or not Hutchinson provides a subnet mask is pure conjecture and speculation. As previously pointed out, inherency may not be established by "'probabilities or possibilities.'" *Continental Can*, supra (quoting *In re Oelrich*, supra).

Rebuttal Response:

In the most recent Response to Arguments provided by the Examiner in their Final Rejection dated February 26, 2008, the Examiner states:

> "it is well-known in the art that in IP-network it is inherent to have a subnet mask … associated with each IP address and since an IP address is assigned to a network card when each network card inherently has a MAC address burned to the hardware itself and therefore any time network card receives the packet or sends the packet as showed in Hutchinson, Fig. 13, <u>all three information goes along together</u>".

Applicants respectfully submit, and as will be shown in detail with documentary evidence provided as attachments hereto, that it is <u>not</u> well-known or inherent to <u>send all three</u> of IP address, MAC address *and subnet mask* in a data packet that is transmitted over an IP-network.

Subnets are used to partition a host address space by assigning subnet numbers to the individually partitioned LANs (see, e.g., "RFC 917" attached hereto as Attachment A). There are two parts to a logical IP address – a network portion and a node portion. An internally maintained subnet mask is used by a router or gateway that interconnects a local/private, partitioned network with the public network in order to translate a local address to a global/public address, where the network bits portion of the logical

IP address are represented in such address at the bit locations where the subnet mask has 1s in them, and the node bits portion of the logical IP address are represented in such IP address at the bit locations where the subnet mask has 0s in them. Therefore, the subnet mask is used to define which bits of the logical IP address are associated with the network-portion, and which bit of the logical IP address are associated with the node-portion. Thus, for example, when a subnet mask of 255.255.255.0 exists for a given subnet, the upper twenty-four bits of the IP address specify the network-portion of the address (one common address being 192.168.0.x) and the lower eight bits specify a particular device/node on this private subnet network (0-256 are typical values) (see, e,g, "Subnetting" attached hereto as Attachment B).

A typical TCP/IP data packet, such as described by the cited reference, includes both a source IP address as well as a destination IP address, but does not include subnet mask information (see, e.g., "TCP/IP Suite attached hereto as Attachment C, and specifically note the figure on page 1). Importantly, because the router/gateway provides address translation from the local/private address to the public address (see, e.g., "Network Address Translation" attached hereto as Attachment D), there is no need or reason to include a subnet mask in normal data packets as such information is internally stored within the router that performs the on-the-fly address translation. The fundamental reason why this is so is that the subnet mask is specific to the local/private networks and is not typically used by *other* local/private networks as the address translation is transparently performed by a router/gateway that uses such network mask that is internally maintained within the router.[1]

However, there is a special circumstance where the subnet mask of one local/private network needs to be known by another local/private network. This special circumstance is a wake-up packet, where a node/device on one local/private network wants/needs to wake-up a node/device on another local/private network. The implementation of the wakeup packet protocol requires specification of the subnet mask in order to awaken a device (Specification page 2, lines 19-30). However, this requires that the system administrator *already know* these requisite subnet masks in order to formulate the wake-up packet (Specification page 2, line 30 – page 3, line 4). One of the fundamental premises of the present invention is to facilitate the automated acquisition of such a subnet mask in order to mitigate these system administrator issues (Specification page 3, lines 5-8). Accordingly, as an expressly provisioned claimed feature, a response is returned to a requestor of host information, and *this response* *<u>includes the subnet mask</u>* (Applicants' Claim 1) – thereby advantageously allowing the requester to subsequently perform the

[1] This is somewhat akin to telephone systems in towns/cities having but a single area code, where the area code is not used when dialing other numbers within the same area code (local call), but the area code is used when dialing other numbers outside the same area code (long distance call).

special wake-up of a device on another network without having to know up-front what the subnet mask is for this another network.

The cited Hutchinson passage at col. 4, lines 16-21 and Figure 7 describes the following:

> "Client 104 then sends out an address resolution protocol (ARP) request containing the IP address (10.0.0.1) of a gateway 116 asking for the corresponding 48-bit Ethernet hardware address, referred to as destination MAC address. Gateway 116 responds with its MAC address, in this example ABCD."

As can be seen, this passage describes a request that includes an IP address (with such IP address having been described in detail above, which is not a subnet mask), and in response a MAC address is returned (a MAC address, as commonly known to those of ordinary skill in the art, is a physical (as opposed to logical) address of a particular node/device, which is not a subnet mask). This client/gateway exchange is *internal to the private network*, so this request/response exchange has no need to use subnet masks as a part of such exchange. Even if subnet masks where used internal to the router in servicing this request (which Applicants deny), there would still be no reason to include a subnet mask in this response as the client is requesting an *actual physical hardware address for the gateway* - which is different from an IP address and associated subnet mask (as described in detail above) - that does not use/require a subnet mask. Thus, it is not inherent that a response returned to a client that is requesting a physical hardware address of a router/gateway includes a subnet mask as it is not needed or desired by the client to address the intra-subnetwork-attached router/gateway. Quite simply, while it may be inherent for a router/gateway to *use* a subnet mask (in performing network address translation between two different networks), it is *not* inherent – or even needed or desired – to *include a subnet mask* in a general purpose IP datagram/packet.

Thus, it is urged that Claim 1 is not anticipated by the cited reference as every element recited in such claim is not identically shown in a single reference, per *In re Bond*, supra.

Applicants initially traverse the rejection of Claims 8 and 15 for similar reasons to those given above with respect to Claim 1. It should be further noted that per the amended features of Claims 8 and 15, the data processing system returns a MAC address for a *different computer* (remote computer), and not a MAC address for itself (data processing system), as taught by the cited reference.

Therefore, the rejection of Claims 1, 8 and 15 under 35 U.S.C. § 102 has been overcome.

II. **35 U.S.C. § 103, Obviousness**

Claims 2, 9 and 16 stand rejected under 35 U.S.C. § 103 as being unpatentable over Hutchison et al. (U.S. Patent No. 7,249,191 B1), hereinafter "Hutchison" in view of Bullman et al. (U.S. Publication No. 2002/0162038 A1), hereinafter "Bullman". This rejection is respectfully traversed.

Applicants initially traverse the rejection of Claim 2 (and similarly for Claims 9 and 16) for reasons given above with respect to Claim 1 (of which Claim 2 depends upon), and urge that the additional cited Bullman reference does not overcome the teaching deficiencies identified above with respect to Claim 1.

Further with respect to Claim 2 (and similarly for Claims 9 and 16), it is urged that none of the cited references teach or suggest the claimed feature of "wherein the *requestor* generates a wake-up packet using the host information and sends the wake-up packet to the remote computer" (emphasis added), with the *requestor* being *the same requestor for which <u>a request for host information was received from</u>*, and where such request (that is received from the requester) includes one of a host name or an Internet Protocol address (per Claim 1). In contrast, per the teachings of Bullman (which is being cited as teaching all features of Claim 2), the PHY device sends a wake-up packet. However, this PHY device is not equivalent to the claimed requestor, since requests that include one of a host name or an Internet Protocol address are not received from this PHY device. Per the features of Claim 2 in combination with Claim 1, *the requestor that generates that wake-up packet using host information is the <u>same</u> requestor that requested the host information.* The combined teachings of the cited reference do not establish a teaching/suggestion of a *same device* that requested host information *also* generates a wake-up packet *<u>using</u> this same (requested) host information.* Therefore, it is further urged that Claim 2 (and similarly for Claims 9 and 16) is not obvious in view of the cited references.

Therefore, the rejection of Claims 2, 9 and 16 under 35 U.S.C. § 103 has been overcome.

III. <u>35 U.S.C. § 103, Obviousness</u>

Claims 3, 6, 7, 10, 13, 14, 17 and 20 stand rejected under 35 U.S.C. § 103 as being unpatentable over Hutchison et al. (U.S. Patent No. 7,249,191 B1), hereinafter "Hutchison" in view of Harrison et al. (U.S. Publication No. 2004/0177133 A1), hereinafter "Harrison". This rejection is respectfully traversed.

Applicants initially traverse the rejection of Claim 3 (and similarly for Claims 10 and 17) for reasons given above with respect to Claim 1 (of which Claim 3 depends upon), and urge that the additional cited Harrison reference does not overcome the teaching deficiencies identified above with respect to Claim 1.

Further with respect to Claim 3, two different items are received from a dynamic host configuration protocol server - (1) a media access control address and (2) a subnet mask. The things that are received from the DHCP host per the cited Harrison reference are 'host configuration parameters, including an IP address for the client', 'an IP address of a DNS server', 'an IP address of a TFTP server', and 'a name of a device configuration boot file'. There is no teaching or suggestion of any type of *<u>subnet mask</u> being returned <u>by a DHCP server</u>.* Accordingly, it is further urged that Claim 3 (and similarly for

Claims 10 and 17) is not obvious in view of the cited references do to these numerous additional missing claimed features, as described above.

Applicants initially traverse the rejection of Claim 6 (and similarly for Claims 13 and 20) for reasons given above with respect to Claim 1 (of which Claim 6 depends upon), and urge that the additional cited Harrison reference does not overcome the numerous teaching deficiencies identified above with respect to Claim 1.

Further with respect to Claim 6, it is urged that none of the cited references teach or suggest the claimed feature of "wherein the data processing system is a domain name server". It should be noted that Claim 6 should not be interpreted in the abstract as merely reciting a generic domain name server. Rather, Claim 6 must be interpreted in the context of Claim 1 (since Claim 6 depends upon Claim 1). Per the features of Claim 6 when interpreted in the context of Claim 1, such claim recites a domain name server that performs each of the steps of 'receiving' (a request for host information from a requestor), 'identifying' and 'returning' (a response to the requestor). The DNS server as described by the cited Hutchinson passage at col. 4, lines 13-15 does not perform these three steps. Rather, such a DNS server is described as being 'somewhere on the internet' that 'returns the 32-bit IP address for WebPages.com'. This DNS server could *not* perform a step of 'identifying a media access control address and a subnet mask using the request' as *it does not have access to this type of information.* The present invention and associated specification description is what is the enabling technology that allows a DNS server to identify this type of information. Prior to the present invention, DNS servers did not have access to media access control addresses and a subnet masks for devices. Thus, the combined teachings of the cited references do not in fact teach or suggest *a DNS server that performs steps of "receiving a request for host information for a remote computer from a requestor wherein the request includes one of a host name or an Internet Protocol address and is received from the requestor", "identifying a media access control address and a subnet mask using the request" and "returning a response to the requestor, wherein the response includes the media access control address and the subnet mask"*, as per the features of Claim 6 in combination with Claim 1. Accordingly, it is further urged that Claim 6 (and similarly for Claims 13 and 20) has been erroneously rejected due to this additional claimed feature which is not taught or suggested by the cited references.

Applicants initially traverse the rejection of Claim 7 (and similarly for Claim 14) for reasons given above with respect to Claim 1 (of which Claim 7 depends upon), and urge that the additional cited Harrison reference does not overcome the numerous teaching deficiencies identified above with respect to Claim 1.

Further with respect to Claim 7 (and similarly for Claim 14), it is urged that none of the cited references teach or suggest the claimed feature of "wherein the media access control address and the subnet mask are stored together in a record for both a name-to-address file and an address-to-name file". In rejecting Claim 7, the Examiner states that all of the features of Claim 7 are taught by Harrison at paragraph [0191]. Applicants show that there, Harrison states:

> "[0191] DNS: Domain Name System--The on-line distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the connected Internet implement a hierarchical namespace that allows sites freedom in assigning machine names and addresses. DNS also supports separate mappings between mail destinations and IP addresses."

As can be seen, this cited passage does not teach any type of storing operation at all. In addition, this cited passage does not teach the storing of a media access control address. In addition, this cited passage does not teach the storing of a subnet mask. As described above with respect to Claim 6, DNS servers (until the present invention) did not have access to this type of information such as media access control address and subnet mask. Thus, the teachings of a DNS server in this cited passage does not teach or otherwise suggest the storing of either a media access control address or a subnet a mask.

Still further, while this cited passage alludes to 'mappings' between mail destinations and IP addresses, such 'mapping' does not teach or suggest both a name-to-address file and an address-to-name file (**two-way mapping**), or the storing of both a media access control address and a subnet mask in both of these (missing) files. Instead, this passage merely describes a **one-way mapping** of human-readable machine names to IP addresses. Thus, it is further urged that Claim 7 (and similarly for Claim 14) has been erroneously rejected, as *none of the numerous features* recited in such claim are taught or suggested by the cited references.

Therefore, the rejection of Claims 3, 6, 7, 10, 13, 14, 17 and 20 under 35 U.S.C. § 103 has been overcome.

IV. 35 U.S.C. § 103, Obviousness

Claims 4, 11 and 18 stand rejected under 35 U.S.C. § 103 as being unpatentable over Hutchison et al. (U.S. Patent No. 7,249,191 B1), hereinafter "Hutchison" in view of Matsuda et al. (U.S. Patent No. 7,039,688 B2), hereinafter "Matsuda". This rejection is respectfully traversed.

Applicants initially traverse the rejection of Claim 4 for reasons given above with respect to Claim 1 (of which Claim 4 depends upon), and urge that the additional cited Matsuda reference does not overcome the teaching deficiencies identified above with respect to Claim 1.

Further with respect to Claim 4, it is urged that none of the cited references teach or suggest the claimed feature of "wherein the dynamic host configuration protocol server obtains the media access control address and the subnet mask from a remote computer when the remote computer requests an address from the dynamic host configuration protocol server". In rejecting Claim 4, the Examiner states that all of the Claim 4 features are taught by Matsuda at Figure 7, Element 704; Col. 12, lines 46-52; Col. 12, lines 66-67; and Col. 13, lines 1-5. Applicants urge that these cited passages make no mention of any type of subnet mask. Rather, a media access control address is described. Because Claim 4 recites both a media access control address as well as a subnet mask (and associated operations being performed on both of these two expressly enumerated items), per the features of Claim 4 the 'media access control address' is a different item/thing from the 'subnet mask'. Therefore, it is not proper to interpret Matsuda's teaching of a media access control address to be both the claimed media access control address and the claimed subnet mask as they are two specific items expressly enumerated in the claim. Restated, if a media access control address were the same as, or a superset of, a subnet mask, then the claim would only need to recite one and not the other. However, they are not the same, and the claim therefore explicitly recites both of these as being separate elements. Quite simply, a teaching of one (media access control address) does not teach or suggest the other (subnet mask). This can also be seen in Applicants' Figure 5, where a DNS record 500 includes *both* a MAC address 502 *and* a subnet mask 504. While it may be true that certain network operations require both of these separate items in order to function properly, the DHCP server operations described by the cited Matsuda reference have no such requirement of using both (e.g., it is typically a network router that is concerned with the subnet mask, as this subnet mask is used during a routing operation – a DHCP server has no such concern or use for a subnet mask). Thus, Matsuda's teaching of a DHCP server using a media access control address does not teach or suggest the claimed subnet mask features of Claim 4. Thus, it is further shown that Claim 4 has been erroneously rejected due to these additional claimed features that are not taught or suggested by the cited references.

Therefore, the rejection of Claims 4, 11 and 18 under 35 U.S.C. § 103 has been overcome.

V. **35 U.S.C. § 103, Obviousness**

Claims 5, 12, 19 and 21 stand rejected under 35 U.S.C. § 103 as being unpatentable over Hutchison et al. (U.S. Patent No. 7,249,191 B1), hereinafter "Hutchison" in view of Bahl. (U.S. Patent No. 6,957,276 B1), hereinafter "Bahl". This rejection is respectfully traversed.

Applicants initially traverse the rejection of Claim 5 (and similarly for Claims 12 and 19) for reasons given above with respect to Claim 1 (of which Claim 5 depends upon), and urge that the additional cited Bahl reference does not overcome the teaching deficiencies identified above with respect to Claim 1.

Further with respect to Claim 5, it is urged that none of the cited references teach or suggest the claimed feature of "wherein the media access control address and the subnet are received from a user submitting the media access control address and the subnet mask and are stored in a data processing system for the data processing system". As can be seen, a *user* is involved in the operations recited in Claim 5. Such manual intervention by a user may be required in certain situations where a DHCP server is not used to dynamically assign an IP address to a device, but instead a static IP address is used (Specification page 12, lines 5-24; page 14, line 29 – page 15, line 10). The manual user intervention features recited in Claim 5 accommodate such a scenario. Accordingly, per the features of Claim 5 the user submits both a media access control address as well as a subnet mask, and both the media access control address and the subnet mask are stored in the data processing system. In rejecting Claim 5, the Examiner states that all of the features of Claim 5 are taught by Bahl at Col. 9, lines 1-9. Applicants urge that there, Bahl states:

> "As illustrated in FIG. 2, when a DHCP client machine 200 initially boots onto the network, it transmits a DHCP DISCOVER 202 to the DHCP server 204 in an attempt to obtain an IP address. The DHCP server 204 analyzes the DISCOVER request 202 to determine the type of IP address to be assigned thereto. The DHCP server 204 analyzes the media access control (MAC) address and the client identifier field for the DHCP client 200 that has sent the DISCOVER request 202."

As can be seen, this cited passage describes a traditional, automatic dynamic IP address assignment being performed by a DHCP server. In contrast, per the features of Claim 5, a manual user operation is claimed, whereby a user submits information that is to be stored in the data processing system. Quite simply, an automated dynamic IP address assignment as described by the teachings of the cited reference does not teach or otherwise suggest any type of manual user operations as provided by the features of Claim 5.

Still further, even assuming arguendo that this cited passage does describe a manual user operation (which Applicants deny), even then there would still be no teaching or suggestion of operations pertaining to both a media access control address as well as a subnet mask. This cited passage only makes mention of a media access control address and a client identifier field. There is no mention of any type of subnet mask. As described above with respect to Claim 4, and as depicted by Applicants' Figure 5, a media access control address and a subnet mask are separate items, and the teaching of one (media access control address) does not teach or suggest the other (subnet mask). Accordingly, it is further urged that Claim 5 (and similarly for Claims 12 and 19) has been erroneously rejected due to the additional claimed features recited in Claim 5 that are not taught or suggested by the cited references.

Still further with respect to Claim 21, the Examiner has provided no reason or explanation of how the references read on the features of Claim 21. The Examiner, in rejecting Claim 21, merely relies on the following statement:

> "Hutchinson et al., Bullman et al., Harrison et al. and Matsuda et al. were cited in previous rejections, the teachings that are applicable, hereby incorporated by reference."

Applicants urged that Claim 21 was newly added in the previous response filed by Applicants on January 21, 2008 and thus has not previously been examined by the Examiner. Hence, the Examiner's mere reliance on the reasoning given in the rejection of Claims 5, 12 and 19 fails to address or discuss the specific features pertaining to newly added Claim 21. Thus, Claim 21 has been erroneously rejected as a proper prima facie obviousness has not been established. In addition, none of the cited references either singularly or in combination teach or suggest the claimed features of "wherein the step of identifying a media access control address and a subnet mask using the request comprises identifying a media access control address and a subnet mask for the remote computer using the request, and wherein the step of returning a response to the requestor comprises returning a response to the requestor, *wherein the response includes the media access control address and the subnet mask for the remote computer*" (emphasis added by Applicants). Thus, it is further shown that Claim 21 has been erroneously rejected.

Therefore, the rejection of Claims 5, 12, 19 and 21 under 35 U.S.C. § 103 has been overcome.

VI. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: May 27, 2008

Respectfully submitted,

/Wayne P. Bailey/

Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants